AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph at page 1, lines 3-9, with the following amended paragraph:

--This invention generally pertains to a system and method for securely signing data about to be stored so that any alteration of the data can be detected before the data are subsequently used, and more specifically, pertains to a system and method for computing a signature stored with the data using a secure key, wherein the signature can securely incorporate a signer identification (ID), so that verification of the signature before enabling a client computing device to access and use the data that were stored ensures that neither the data nor the signer ID has been altered [[,]].--

Please replace the paragraph at page 13, lines 24-32, with the following amended paragraph:

--FIGURES 3A and 3B illustrate different aspects of the gaming environment. In FIGURE 3A, a schematic diagram 280 shows that the gaming environment comprises a plurality of fame consoles 284a-284h, which are connected to a gaming server [[282a]] 282. Data packets are conveyed between the gaming server and the game consoles through VPN tunnels, over Internet 285. Each game console 284a-284h is thus connected in secure communication with gaming server 282, which as shown in FIGURE 3B may comprise a single server 282a, or alternatively and more likely, will include a plurality of servers 283 that are coupled together to carry out specific functions required for the gaming service. Use of the VPN tunnel insures a secure connection link between--

Please replace the paragraph at page 14, lines 22-32, with the following amended paragraph:

--As indicated in a flow chart 300 in FIGURE 4, a client 302 initiates the process in a step 306. The client sends the data to be signed to a server 304 in a step 308. The server receives the data in a step 310 and computes a signature by applying a key known only to the server in a step 312. In a preferred embodiment, the server computes the signature using a Keyed-Hash Message Authentication Code (HMAC). The HMAC technique for signing a document is described in Federal Information Processing Standards Publication 198, published march 6, 2002, which notes that HMACs typically have two functionally distinct parameters, including a message input and a secret key that is known only to the message originator and intended receiver(s). However, the present invention uses the HMAC in a different manner, and the key is not [[know]] known to any client, but is only known on the server. The HMAC employs the secret key in--

Please replace the paragraph at page 18, lines 1-6, with the following amended paragraph:

--decision step 462, the server compares the signer ID from the compound signature to a list of banned signer IDs. If the signer ID is on the list [[(because]] because of some infraction that caused the client (or user of the client game console) to be banned from playing the game for which the data were saved, the server sends a negative result to the client in a step 470; otherwise, the server computes a temporary signature from the temporary digest in a step 464, using the same algorithm and secret used during the data signing process.--